(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号

特開平9－307542

(43)公開日　平成９年(1997)11月28日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｈ０４Ｌ　9/08			Ｈ０４Ｌ　9/00	６０１Ｂ	
Ｇ０９Ｃ　1/00	６３０	7259－5Ｊ	Ｇ０９Ｃ　1/00	６３０Ｂ	
		7259－5Ｊ		６３０Ｅ	
			Ｈ０４Ｌ　9/00	６０１Ｅ	

審査請求　未請求　請求項の数８　ＯＬ　（全 16 頁）

(21)出願番号　特願平8－154688

(22)出願日　平成８年(1996)６月14日

(31)優先権主張番号　特願平8－59746

(32)優先日　平８(1996)３月15日

(33)優先権主張国　日本（ＪＰ）

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号

(72)発明者　浅野　智之
東京都品川区北品川６丁目７番35号　ソニー株式会社内

(72)発明者　石井　眞
東京都品川区北品川６丁目７番35号　ソニー株式会社内

(72)発明者　窪田　一郎
東京都品川区北品川６丁目７番35号　ソニー株式会社内

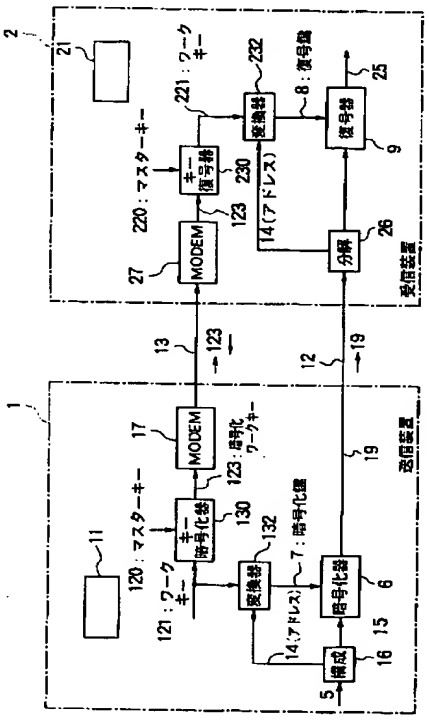
(74)代理人　弁理士　佐藤　隆久

(54)【発明の名称】　データ伝送装置とその方法

(57)【要約】

【課題】　暗号鍵または復号鍵の伝送の安全性を高めて、暗号化伝送データの漏洩に対する安全性を高めるデータ伝送装置を提供する。

【解決手段】　大容量のデータを伝送する衛星回線伝送路などの大容量伝送路１２と、暗号鍵または復号鍵あるいはこれらの生成のための情報を伝送する公衆電話回線などの小容量伝送路１３を設ける。暗号化セッション鍵をワークキーと送信先の受信装置２の宛先アドレスとを用いて変換する。また復号用セッション鍵を自己のアドレスとワークキーを用いて変換する。ワークキーは好ましくは、暗号化されて小容量伝送路１３を伝送される。送信装置１において、伝送すべきデータ５を上記のごとく変換した暗号セッション７を用いて暗号化する他、宛先データなどの伝送制御情報を付加して大容量伝送路１２を経由して受信装置２に伝送する。受信装置２において、上記のごとく変換した復号セッション鍵８を用いて暗号化データ１９を復号する。



1

【特許請求の範囲】

【請求項１】大量のデータを高速で伝送可能な第１の伝送系統と、

有線形式の第２の伝送系統と、

前記第１の伝送系統と前記第２の伝送系統を介して接続されている第１の伝送装置と第２の伝送装置とを有し、

前記第１の伝送装置が前記第２の伝送系統を介して復号化セッション鍵を生成するためのワークキーを前記第２の伝送装置に伝送し、

前記第１の伝送装置が、暗号化データを送信する前記第２の伝送装置の宛先データおよび前記暗号化セッション鍵を生成するためのワークキーを用いて暗号化セッション鍵を生成し、該生成した暗号化セッション鍵を用いて伝送データを暗号化し、前記宛先データを付加して前記第１の伝送系統に送出し、

前記第２の伝送装置は前記第１の伝送系統から受信したデータから前記宛先データを取り出し、該宛先データと前記第２の伝送系統から受信した暗号化セッション鍵を生成するためのワークキーとから復号化セッション鍵を生成し、該生成した復号化セッション鍵を用いて前記暗号化伝送データを復号するデータ伝送装置。

【請求項２】前記宛先アドレスは複数の装置のグループを示すアドレスである、請求項１記載のデータ伝送装置。

【請求項３】前記第１の伝送系統は衛星回線伝送路である、請求項１または２記載のデータ伝送装置。

【請求項４】前記第１の伝送装置は、前記第２の伝送系統を介して前記第２の伝送装置に伝送する、復号化セッション鍵を生成するためのワークキーを暗号化して伝送し、

前記第２の伝送装置は、該暗号化されている復号化セッション鍵を生成するためのワークキーを復号し、該復号したワークキーと前記宛先データを用いて復号化セッション鍵を生成する請求項１～３いずれか記載のデータ伝送装置。

【請求項５】大量のデータを高速で伝送可能な第１の伝送系統および有線形式の第２の伝送系統に接続され、

ワークキーを前記第２の伝送系統に送出する第１の送出手段と、

ワークキーと送信先のアドレスとから暗号化セッション鍵を生成する鍵変換手段と、

前記生成した暗号化セッション鍵を用いて伝送すべきデータを暗号化するデータ暗号化手段と、

該暗号化伝送データに、送信先のアドレスを付加して前記第１の伝送系統に送出する送出手段とを有するデータ伝送装置。

【請求項６】大量のデータを高速で伝送可能な第１の伝送系統と、有線形式の第２の伝送系統とを用いて第１の伝送装置と第２の伝送装置との間で暗号化データを伝送するデータ伝送方法であって、

2

前記第２の伝送系統を介して復号化セッション鍵を生成するためのワークキーを前記第２の伝送装置に伝送し、

暗号化データを送信する前記第２の伝送装置の宛先データおよび前記暗号化セッション鍵を生成するためのワークキーを用いて暗号化セッションキー鍵を生成し、該生成した暗号化セッション鍵を用いて伝送データを暗号化し、前記宛先データを付加して前記第１の伝送系統に送出し、

前記第１の伝送系統から受信したデータから前記宛先データを取り出し、該宛先データと前記第２の伝送系統から受信した暗号化セッション鍵を生成するためのワークキーとから復号化セッション鍵を生成し、該生成した復号化セッション鍵を用いて前記暗号化伝送データを復号するデータ伝送方法。

【請求項７】前記宛先アドレスは複数の装置のグループに対するアドレスである、請求項６記載のデータ伝送方法。

【請求項８】大量のデータを高速で伝送可能な第１の伝送系統と、

有線形式の第２の伝送系統と、

前記第１の伝送系統と前記第２の伝送系統を介して接続されている第１の伝送装置と第２の伝送装置とを有し、

前記第１の伝送装置が前記第２の伝送系統を介して復号化セッション鍵を生成するためのワークキーを前記第２の伝送装置に伝送し、

前記第１の伝送装置が、前記暗号化セッション鍵を生成するためのワークキーを用いて暗号化セッション鍵を生成し、該生成した暗号化セッション鍵を用いて伝送データを暗号化し、前記宛先データを付加して前記第１の伝送系統に送出し、

前記第２の伝送装置は前記第２の伝送系統から受信した暗号化セッション鍵を生成するためのワークキーとから復号化セッション鍵を生成し、該生成した復号化セッション鍵を用いて前記暗号化伝送データを復号するデータ伝送装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明はデータを伝送するデータ伝送装置とその方法に関するものであり、特に、大量のデータを暗号化して送受信する場合に用いる暗号鍵および復号鍵の管理を適切に行うデータ伝送装置とその方法に関する。

【０００２】

【従来の技術】公衆電話回線、専用回線などを用いてデータ伝送する場合または通話する場合、伝送情報の漏洩を防止するためまたは伝送情報に対する攻撃（妨害）に対して情報の信頼性を維持するため、平文のデータを暗号化し（スクランブルし）て伝送し、受信先で暗号化されたデータを復号して（デスクランブルして）いる。代表的な暗号方式としては共通鍵暗号方式と公開鍵方式と

が知られている。共通鍵暗号方式は対称暗号系とも呼ばれており、アルゴリズム非公開型とアルゴリズム公開型とが知られている。アルゴリズム公開型の代表的なものとしてＤＥＳ（Data Encryption Standard）が知られている。公開鍵方式は、検査鍵から生成鍵を導出するために莫大な計算量が必要なため実質的に生成鍵が解読されないので、暗号鍵を公開してもよい暗号方式であり、非対称鍵暗号方式とも呼ばれている。

【０００３】暗号化方式は伝送データが伝送される回線系統の種別、伝送データの機密度（秘密性）、伝送データの量などに応じて決定される。専用回線を用いたデータ伝送においては、情報の漏洩、伝送データへの攻撃の度合いは低いが、公衆電話回線を用いてデータ伝送する場合は情報の漏洩の度合い、攻撃の度合いは高くなる。さらに衛星放送回線を用いたデータ伝送は、不特定多数の装置で受信可能であるから情報の漏洩の度合いは一層高くなる。

【０００４】図１は伝送路上のデータを共通鍵暗号化方式で暗号化する暗号化データ伝送装置の一例を示す概略構成図である。図１の暗号化データ伝送装置において、符号１は送信装置（送信者）を示し、２は受信装置（受信者）を示し、３は盗聴装置（盗聴者）を示し、４はデータ伝送路を示し、５は伝送すべきデータを示し、６は送信装置１内に設けられた暗号化器を示し、７は暗号化器６で暗号化に用いる暗号化鍵（暗号化用セッションキーという）を示し、８は復号鍵（復号用セッションキーという）を示し、９は復号鍵を用いてデータ伝送路４から受信した暗号化データを復号する復号器を示し、１０は復号後のデータを示す。送信装置１において、データ５を伝送路４上に送出する際に、暗号化器６において暗号化鍵７を用いてデータ５を暗号化し、暗号化したデータを伝送路４を経由して受信装置２に送出する。受信装置２において、伝送路４から暗号化されたデータを受信したら、復号器９において暗号鍵７に対応する復号鍵８を用いて受信した暗号化されたデータを復号し、目的とする復号（解読）データ１０を得る。この例においては、盗聴装置３が伝送路４から受信装置２と同様に暗号化されたデータを受信しても、復号鍵８がないのでこれを正しく復号することが困難である。すなわち、盗聴装置３ではそのままでは意味不明のスクランブルのかかったデータを扱うことになるから、現実的に盗聴装置３側に情報が漏洩することを防いでいる。この例における共通鍵暗号方式の主要な暗号化方式では、一般に暗号化鍵と復号鍵は同一のビット列である。

【０００５】最近、特定の契約者との間にのみＴＶ番組を提供する衛星放送が行われている。衛星放送に用いる伝送系統は、映像と音声という大量のデータ（情報）を短時間で伝送することが可能である。また人工衛星を用いた伝送系統は、大量の情報を短い時間で伝送することが可能であるため、放送に限らず、コンピュータ・データなどのデータの伝送に広く利用されている。しかしながら、人工衛星を用いた伝送においては、電話回線、専用回線などの１対１通信方式と異なり、不特定多数の多くの受信者が（受信装置で）容易に受信できるので、盗聴されやすいという面も有している。その結果、たとえば、有料衛星放送が盗聴される可能性が高い。そこで、ＴＶ放送の映像データ、音声データについても暗号化して伝送することが提案されている。実際の伝送においては全てのデータについて暗号化処理をする訳ではなく、送信装置において伝送すべきデータの内容に応じて、暗号化すべきデータを暗号化して伝送路上に送出し、受信者は暗号化されたデータの全部または一部を復号し、その結果得られた情報により、現在その全部または一部が復号されたデータが自分にとって必要なものであるか否かを知る。

【０００６】このように暗号化したデータを伝送する暗号化データ伝送装置において、送信側と受信側とで、事前に暗号鍵と復号鍵を秘密に持つ必要がある。送信側で暗号鍵を持ち受信側で復号鍵を持つ従来の方法としては、たとえば、衛星回線伝送路を用いて映像データなどを暗号化して伝送する場合には、送信者が受信者に復号鍵を記録した紙やＩＣカード等を郵送等の方法で送る方法と、衛星回線伝送路を暗号鍵と復号鍵を伝送する方法、さらにこれらを組み合わせた方法が考えられる。

【０００７】

【発明が解決しようとする課題】暗号鍵と復号鍵の従来の管理方法には下記に挙げる問題がある。第１の問題は、送信者による暗号化鍵の所有のしかた、あるいは受信者による復号鍵の所有のしかたに関係した問題である。上述したように、送信者が暗号化鍵を持ち受信者が復号鍵を持つための方法としては、送信者が受信者に復号鍵を記録した紙、ＩＣカードなどの物体を郵送等の方法で送る方法と、衛星回線伝送路を用いて送る方法、さらにこれらを組み合わせた方法が一般的である。

（１）復号鍵を記録した物体を郵送等で送る方法においては、その手続きの繁雑さから暗号化鍵および復号鍵の変更が容易に行えない。そのため多くのデータに対して同一の鍵を用いて暗号化したデータを伝送路上に送出することになり、盗聴者により多くの情報を与えるという意味で、暗号解読に対しての安全性が低い。

（２）復号鍵を衛星回線伝送路を用いて送る方法においては、衛星回線伝送路上のデータは、その者を送信者が受信者として希望するか否かにかかわらず、アンテナ等の機材を持つ不特定多数の者に受信されることから、送信者が希望する受信者以外の者に復号鍵を知られてしまう可能性があるので、伝送の安全が保てないという課題がある。

（３）上記２つの方法を組み合わせる方法、つまり、郵送等で送られた物体に記録してある情報と、衛星回線伝送路を伝送された情報から復号鍵を作成する方法におい

ては、２つの方法の欠点が補われ、この伝送方法の安全性はある程度強いものになる。しかし、たとえば、衛星回線伝送路上のデータを受信でき、かつ、郵送等で他人に送られた情報をなんらかの方法で知りえた者は、この他人が用いる復号鍵を知り、暗号化されている衛星回線伝送路上の他人宛のデータの復号ができることになり、依然として情報が漏洩するという問題がある。

【０００８】第２の問題は送信者がデータを暗号化するか否かを、あるいは、受信者が受信したデータを復号するか否かをいかにして判断するかに関する。上述したように、現在一般的に用いられている方法では、送信装置においてデータの内容を見て暗号化する必要のあるデータを暗号化して伝送路上に送信し、受信装置においては伝送路から受信した暗号化されたデータの全部または一部を復号して得られた情報により、このデータが自分にとって必要であるか否かを判断する。しかしこの方法では、送信装置において、データが暗号化する必要のあるものか否かを知るためにその内容を知るための処理と、受信装置において受信した暗号化されたデータは自分の必要とするものであるか否かを判断するために暗号化されたデータの全部または一部を復号するための処理が必要である。そのためにはより高速に伝送を行う必要があるが、これまでの装置構成ではその要望を満足できなかった。

【０００９】本発明の目的は、送信側において有効に伝送データを暗号化し、受信側において伝送された暗号化データを有効に復号できるデータ伝送装置とその方法を提供することにある。

【００１０】

【課題を解決するための手段】本発明においては、送信側が、ワークキーとを用いて暗号化セッション鍵を生成する、好適には、受信側の宛先アドレスとワークキーとを用いて暗号化セッション鍵を生成して、その鍵を用いて伝送データを暗号化して、第１の伝送系統を介して送出する。送信側から受信側に第２の伝送系統を介してワークキーを伝送しておく。受信側では、ワークキーを用いて、または好適には宛先アドレスとワークキーとを用いて復号化セッション鍵を生成し、この鍵を用いて伝送データを復号する。本発明は、第２の課題を解決するために、送信者がデータを暗号化するか否かを、あるいは、受信者が受信したデータを復号するか否かを、データを伝送するための制御情報によって判断する。本発明においては、大量のデータを高速かつ効率よく伝送可能な衛星放送伝送系統（伝送路）などの大容量伝送路（第１の伝送系統）と、この大容量伝送路とは独立に、ワークキーの授受を行う公衆電話回線などの小容量伝送路（第２の伝送系統）を用いる。小容量伝送路としては、漏洩に対する機密性を高めるため、送信装置と受信装置との間の通信が１対１で行える有線通信路が好ましい。

【００１１】したがって、本発明によれば、大量のデータを高速で伝送可能な第１の伝送系統と、有線形式の第２の伝送系統と、第１の伝送系統と第２の伝送系統を介して接続されている第１の伝送装置と第２の伝送装置とを有し、第１の伝送装置が第２の伝送系統を介して復号化セッション鍵を生成するためのワークキーを第２の伝送装置に伝送し、第１の伝送装置が、暗号化データを送信する第２の伝送装置の宛先データおよび前記暗号化セッション鍵を生成するためのワークキーを用いて暗号化セッション鍵を生成し、該生成した暗号化セッション鍵を用いて伝送データを暗号化し、宛先データを付加して第１の伝送系統に送出し、第２の伝送装置は第１の伝送系統から受信したデータから宛先データを取り出し、該宛先データと第２の伝送系統から受信した暗号化セッション鍵を生成するためのワークキーとから復号化セッション鍵を生成し、該生成した復号化セッション鍵を用いて暗号化伝送データを復号するデータ伝送装置が提供される。宛先アドレスとしては、単一の装置を示す場合に限らず、複数の装置のグループを示すこともできる。

【００１２】好適には、第１の伝送系統は衛星回線伝送路である。また好適には、第１の伝送装置は、第２の伝送系統を介して第２の伝送装置に伝送する、復号化セッション鍵を生成するためのワークキーを暗号化して伝送し、第２の伝送装置は、該暗号化されている復号化セッション鍵を生成するためのワークキーを復号し、該復号したワークキーと前記宛先データを用いて復号化セッション鍵を生成する。

【００１３】また本発明によれば、大量のデータを高速で伝送可能な第１の伝送系統および有線形式の第２の伝送系統に接続され、ワークキーを第２の伝送系統に送出する第１の送出手段と、ワークキーと送信先のアドレスとから暗号化セッション鍵を生成する鍵変換手段と、生成した暗号化セッション鍵を用いて伝送すべきデータを暗号化するデータ暗号化手段と、該暗号化伝送データに、送信先のアドレスを付加して第１の伝送系統に送出する送出手段とを有するデータ伝送装置が提供される。

【００１４】さらに本発明によれば、大量のデータを高速で伝送可能な第１の伝送系統と、有線形式の第２の伝送系統とを用いて第１の伝送装置と第２の伝送装置との間で暗号化データを伝送するデータ伝送方法であって、第２の伝送系統を介して復号化セッション鍵を生成するためのワークキーを第２の伝送装置に伝送し、暗号化データを送信する第２の伝送装置の宛先データおよび暗号化セッション鍵を生成するためのワークキーを用いて暗号化セッションキー鍵を生成し、該生成した暗号化セッション鍵を用いて伝送データを暗号化し、宛先データを付加して第１の伝送系統に送出し、第１の伝送系統から受信したデータから宛先データを取り出し、該宛先データと第２の伝送系統から受信した暗号化セッション鍵を生成するためのワークキーとから復号化セッション鍵を生成し、該生成した復号化セッション鍵を用いて暗号化

伝送データを復号する、データ伝送方法が提供される。

【００１５】

【発明の実施の形態】

【実施例１】本発明のデータ伝送装置の第１実施例について、図２を参照して述べる。図２は本発明のデータ伝送装置の第１実施例の概念的な構成図である。図２に図解した第１実施例のデータ伝送装置において、符号１は送信装置（送信者、または第１の伝送装置）を示し、２は受信装置（受信者または第２の伝送装置）を示し、３は送信装置１および受信装置２を除く第３者の受信装置を示し、１２は第１の伝送系統としての大容量伝送路を示し、１３は第２の伝送系統としての小容量伝送路を示す。

【００１６】本発明においては、大容量伝送路１２を介してＴＶ信号、コンピュータデータなどの大量のデータを伝送する。大容量伝送路１２としては、大量のデータを高速かつ効率よく伝送する衛星回線伝送路が好ましい。また、暗号または復号に関する情報を伝送する小容量伝送路１３としては、衛星回線伝送路より情報の漏洩が少ない１対１通信を行う、有線伝送路、たとえば、公衆電話回線、専用回線などが望ましい。以下の実施例においては、小容量伝送路１３として公衆電話回線を用いた場合を例示する。

【００１７】図３は大容量伝送路１２として衛星回線伝送路を用い、小容量伝送路１３として公衆電話回線を用いた伝送路の概略構成を示す図である。衛星回線伝送路１２は、送信用アンテナ１２０、空中伝送路１２１、中継器を内蔵した人工衛星１２２、空中伝送路１２３、および、受信用アンテナ１２４から構成されている。送信用アンテナ１２０には、送信装置１に設けられた送信機（ＴＸ）１０が接続され、受信用アンテナ１２４には受信装置２に設けられた受信機（ＲＸ）２０が接続されている。受信機２０としては、たとえば、ＴＶ映像信号を受信する場合は、ＴＶ受像機内の受信機である。なお、アンテナ１２０、１２４は送信用だけでなく受信用にも用いることができる。送信装置１内の送信機（ＴＸ）１０、受信装置２内の受信機（ＲＸ）２０はそれぞれ送受信機として、送信も受信も可能な装置を設けることができる。特に、大容量伝送データとして、コンピュータデータを伝送する場合などは、相互に送受信する場合が多いから、送信装置１および受信装置２にそれぞれ送受信機を設けておくことが望ましい。公衆電話回線１３は、送信装置１内に変復調器（ＭＯＤＥＭ：モデム）１７を設け、受信装置２内にも変復調器（モデム）２７を設けておき、これら変復調器１７，２７相互で、電話線１３１、交換機（ＥＸ）１３０、電話線１３２を介して暗号鍵などのデータの伝送を行う。以下、大容量伝送路１２としては、図３に図解した衛星回線伝送路１２、小容量伝送路１３として図３に示した公衆電話回線１３を例示する。

【００１８】送信装置１が大容量伝送路１２に送出した暗号化したデータを、大容量伝送路１２と無線接続されている受信装置２に送信する。本実施例においては、送信装置１は大容量伝送路１２を用いて、伝送すべきデータをインターネット・プロトコル（INTERNET Protocol：インターネット通信規約）ＩＰを用いて伝送する。なお通信規約としては、インターネット・プロトコルＩＰに限らず、後述するように、たとえば、ＡＴＭ（Asynchronous Transfer Mode、非同期転送モード）など、その他の通信規約を用いることもできる。ただし、以下の実施例においては、インターネット・プロトコルＩＰについて例示する。インターネット・プロトコルＩＰは、データの伝送における代表的なプロトコルであり、その詳細はたとえば、西田竹志著の文献、ＴＣＰ／ＩＰ　インターネットワーキング、株式会社、ソフト・リサーチ・センター発行、に示されている。

【００１９】図４はインターネット・プロトコルＩＰにおけるメッセージ伝送の単位であるＩＰデータグラム１５の概略図である。符号５は伝送すべきデータを示し、１４はＩＰヘッダを示し、１５はメッセージ伝送の１単位であるＩＰデータグラムを示す。インターネット・プロトコルＩＰに従えば伝送すべきデータ５に、伝送に必要な制御情報であるＩＰヘッダ１４が付加され、全体がＩＰデータグラム１５を構成する。本実施例においては、ＩＰヘッダ１４には、送信装置１からデータを伝送する宛先データ（すなわち、受信装置２の宛先データ）、および、伝送すべきデータ５を暗号化するか否かのフラグがセットされる。ＩＰヘッダ１４に規定される宛先データおよび暗号化するか否かの情報を伝送制御情報と呼ぶ。

【００２０】データ伝送装置の構成

図５は図２に図解した本発明の暗号化データ伝送装置の第１実施例についてインターネット・プロトコルＩＰを適用して実現したより詳細な構成を示す図である。暗号化データ伝送装置は、大容量伝送路１２（具体的には、図３に図解した大容量伝送路１２）と小容量伝送路１３（具体的には、図３に図解した公衆電話回線１３）を介して接続されている送信装置１と受信装置２とを有している。送信装置１には、図４に図解したように伝送すべきデータ５にＩＰヘッダ１４を付加してＩＰデータグラム１５を形成するＩＰデータグラム構成器１６と、暗号鍵７を用いてＩＰデータグラム１５を暗号化して暗号化データ１９を生成する暗号化器６が設けられている。衛星回線伝送路１２には、図示しない送信機１０（図３参照）を用いて暗号化器６で暗号化された暗号化データ１９とＩＰデータグラム構成器１６から出力されて暗号化されていない平文データ１８とが伝送される。送信装置１にはさらに、公衆電話回線１３を介して復号鍵の伝送を行う変復調器（モデム）１７と、送信装置１内の信号処理および制御処理を行う信号処理装置１１とが設けら

れている。信号処理装置１１は、たとえば、コンピュータを用いて構成されている。信号処理装置１１はＩＰデータグラム構成器１６、暗号化器６および変復調器（モデム）１７の全体処理および制御を行う。受信装置２には、データグラム分解器２６、復号器９、信号処理装置２１、変復調器（モデム）２７が設けられている。

【００２１】送信装置１の動作

送信装置１において、ＩＰデータグラム構成器１６が伝送すべきデータ５にＩＰヘッダ１４を付加してＩＰデータグラム１５を生成する。この際に、送信装置１の信号処理装置１１はＩＰヘッダ１４中の宛先アドレスの部分を用いて、伝送データ５を暗号化するか否かを判断し、暗号化する場合には、ハードウェアとして構成された暗号化器６を用いて暗号化鍵（暗号化用セッションキー）７を鍵として伝送すべきデータ５を暗号化し、暗号化データ１９を衛星回線伝送路１２に送出する。なお、暗号鍵７は、送信装置１内の信号処理装置１１が上記宛先アドレスに基づいて生成する。伝送データ５を暗号化しない場合には、送信装置１は暗号化されていないＩＰデータグラム（平文データ）１８を衛星回線伝送路１２に送出する。

【００２２】図６は、上記の送信装置の主要な処理の流れを示すフローチャートである。ステップＳ１において送信装置１のＩＰデータグラム構成器１６は伝送すべきデータ５にＩＰヘッダを付加してＩＰデータグラムを生成する。ステップＳ２において、送信装置１の暗号化器６はＩＰヘッダ１４に含まれる宛先アドレスを見てデータを暗号化するか否かを判断する。暗号化する場合にはステップＳ３へ進み、暗号化器６は暗号鍵７を用いて伝送すべきデータ５に対して暗号化処理を行う。その後、ステップＳ４へ進み、送信装置１の送信機１０（図示せず）は暗号化したデータを衛星回線伝送路１２に送出する。暗号化しない場合には、ステップＳ４に進み、送信装置１の送信機１０（図示せず、図３参照）は暗号化しない平文データ１８を衛星回線伝送路１２に送出する。信号処理装置１１はこれらの動作処理および制御を行う。

【００２３】復号鍵８の伝送

衛星回線伝送路１２を用いたデータの伝送とは別に、公衆電話回線１３を用いて、信号処理装置１１と変復調器（モデム）１７、および、信号処理装置２１と変復調器（モデム）２７との間で、送信装置１から受信装置２に暗号鍵７に対応する復号鍵８を伝送しておく。これにより、暗号鍵７に対応した復号鍵８を用いれば受信装置２において暗号化データ１９の復号が可能になる。

【００２４】受信装置２の動作

受信装置２において、図示しない受信機２０（図３参照）で衛星回線伝送路１２から受信した、平文データ１８および暗号化データ１９をＩＰデータグラム分解器２６に入力する。ＩＰデータグラム分解器２６は、受信データからＩＰヘッダ１４を分離し、この中の宛先アドレスを見て、このデータが自分宛のものか否かと、復号すべきか否かを調べる。このデータが自分宛のものである場合には、ＩＰデータグラム分解器２６はＩＰヘッダ１４を除いた受信データ２９を後段の回路、たとえば、暗号化データについては復号器９、および、平文データについては図示しない回路に送出する。復号すべき場合には、ハードウェアとして構成されている復号器９が復号鍵（復号用セッションキー）８を用いて、ＩＰヘッダ１４を分離した後の暗号化データ２９を、送信装置１における伝送すべきデータ５に相当するもとのデータ２５に復号する。衛星回線伝送路１２から受信したデータが自分宛のものであり、復号する必要のない平文である場合には、ＩＰデータグラム分解器２６はＩＰヘッダ１４を分離し、その後、復号鍵を用いて復号することなく、平文データ２８として送信装置１における伝送すべきデータ５に相当するもとの送信データを取り出す。

【００２５】図７は図５に示した受信装置２における動作処理の流れを示すフローチャートである。ステップＳ５で、受信装置２のＩＰデータグラム分解器２６は図示しない受信機（図３参照）で受信した平文データ１８および暗号化データ１９のＩＰデータグラム１５からＩＰヘッダ１４を取り出す。平文データ１８からＩＰヘッダ１４を除いてデータを平文データ２８とし、暗号化データ１９からＩＰヘッダ１４を除いてデータを暗号化データ２９とする。ステップＳ６で、信号処理装置２１はＩＰヘッダ１４の宛先アドレスを見て自分宛のデータであるかどうか判断する。自分宛のデータでない場合には受信装置２は処理を終了する。宛先アドレスが自分宛のデータである場合には、ステップＳ７に進み、信号処理装置２１はＩＰヘッダ１４を見て、暗号化データ２９を復号鍵８を用いて復号するか否かを判断する。復号鍵８を用いて暗号化データ２９を復号する場合にはステップＳ８に進み、信号処理装置２１は復号器９において復号鍵８を用いた復号処理を行なわせ、その後、ステップＳ９においてデータを取り出す。ステップＳ７において復号鍵８を用いて復号しない場合には、ステップＳ９に進み、信号処理装置２１は平文データ２８を取り出す。

【００２６】第１実施例の効果

映像・音声（ＡＶ）データ、あるいは、コンピュータデータなどの大容量のデータが衛星回線伝送路などの大容量伝送路１２を介して、必要に応じて、暗号化されて伝送される。暗号化されたＡＶデータは公衆電話回線などの小容量伝送路１３を介して事前に復号鍵８を送信装置１から送付されている受信装置２でしか有効に復号できない。したがって、図２に示した、有効に復号鍵８が授与されていない受信装置３において、仮に衛星回線伝送路１２を介して暗号化データ１９を受信したとしても意味のないデータを受信したことになり、実質的に第３者としての受信装置３（図２参照）における盗聴（盗用）

が防止できる。暗号鍵７に対応する復号鍵８は公衆電話回線などの衛星回線伝送路に比較して機密性の高い有線の小容量伝送路１３を介して伝送されるから、盗用者が大容量伝送路１２のみ監視していても、復号鍵８は判らない。したがって第３者としての受信装置３（図２参照）において衛星回線伝送路１２からのデータを受信したとしても、そのデータが暗号化されていれば、有効に復号できず、事実上、盗聴されたことにならない。特に、公衆電話回線などの小容量伝送路１３は送信装置１と受信装置２との間で１対１の伝送を行う有線路であるから、盗聴を意図した受信装置３（図２参照）においては接続されず、衛星回線伝送路などの大容量伝送路１２に比較して、盗聴または漏洩は起こりにくい。

【００２７】

【実施例２】本発明のデータ伝送装置の第２実施例を述べる。図８は本発明の第２実施例としてのデータ伝送装置の概略構成図である。図８に図解したデータ伝送装置は、１台の送信装置１に対して２台の受信装置２Ａ，２Ｂがそれぞれ衛星回線伝送路などの大容量伝送路（第１の伝送系統）１２および公衆電話回線などの小容量伝送路（第２の伝送系統）１３を介して接続されている。受信装置３は、図２に図解した場合と同様、送信装置１とは正規に接続しない受信装置３である。大容量伝送路１２および小容量伝送路１３の構成は、図３に図解した構成と同様である。第２実施例においては、送信装置１から２台の受信装置２Ａ，２Ｂに対して小容量伝送路１３を介して復号鍵（復号用セッションキー）と、大容量伝送路１２を用いる伝送において使用する宛先アドレスを伝送する。受信装置２Ａに対する宛先アドレスと受信装置２Ｂに対する宛先アドレスとは異なる。したがって、受信装置２Ａまたは２Ｂは自己に対する伝送か否かを宛先アドレスを検査することによって識別できる。送信装置１と受信装置２Ａ、または、送信装置１と受信装置２Ｂとのデータ伝送は、それぞれ、第１実施例と同じである。第２実施例によれば、大容量伝送路１２を用いて、同時に複数、本実施例は２台の受信装置２Ａ，２Ｂに暗号化データを伝送し、それぞれの受信装置で復号できる。もちろん、ＩＰヘッダ１４の伝送制御情報の暗号化するか否かを示すフラグがセットされていない場合は暗号化しないデータを伝送することもできる。

【００２８】第２実施例の変形例

上述した第２実施例においては、２台の独立した宛先アドレスを有する受信装置２Ａ，２Ｂが、同時に大容量伝送路１２を介して暗号化データを受信でき、宛先アドレスが一致する受信装置が有効に暗号化データを復号する場合について述べたが、本実施例の変形態様としては、２台の受信装置２Ａ，２Ｂの宛先アドレスを同じにして、２台の受信装置２Ａ，２Ｂが同時に暗号化データを受信し、２台の受信装置の両者で暗号化データを復号可能にすることもできる。このような運用の例としては、たとえば、ある企業の本社から複数の支部に同じ暗号化データを伝送する場合、複数の支店ごとに伝送することなく、１度で全ての支店に伝送する場合などがある。すなわち、伝送回数を少なくできるという利点がある。また、有料映像データを暗号化して多くの有料放送加盟者に伝送する場合なども、有料放送加盟者側の受信装置の宛先アドレスを同じにしておけば、それらの複数の受信装置に暗号化された有料映像データを１度伝送するだけで、有効な受信装置側で復号できる。

【００２９】

【実施例３】本発明のデータ伝送装置の第３実施例を述べる。第３実施例のデータ伝送装置の構成は、図２、図５および図８を参照して述べた第１実施例および第２実施例のデータ伝送装置の構成と同様である。ただし、第１実施例および第２実施例においては、大容量伝送路１２から暗号化データを伝送する前に、送信装置１から受信装置２に復号鍵（復号用セッションキー）を小容量伝送路１３を介して伝送したが、第３実施例においては、受信装置２から送信装置１に小容量伝送路１３を介して事前に暗号化鍵（暗号化用セッションキー）を伝送しておく。この暗号化鍵は、受信装置２において大容量伝送路１２を用いたデータ伝送において使用する受信装置２の宛先アドレスに基づいて生成される。受信装置２において、暗号鍵に対応する復号鍵は判っている。送信装置１において伝送データを暗号化する場合には、この暗号化鍵を用いて暗号化処理を行う。暗号化データ伝送およびその復号処理は、第１実施例および第２実施例と同様である。第３実施例においては、受信装置２が送信装置１に対して暗号化鍵を指定することができる。

【００３０】

【実施例４】本発明のデータ伝送装置の第４実施例を述べる。図９は本発明のデータ伝送装置の第４実施例の構成図である。送信装置１と受信装置２とは大容量伝送路１２と小容量伝送路１３を介して接続されている。これらの接続状態は図３に図解した接続状態と同様である。送信装置１は、小容量伝送路１３に接続された変復調器（モデム）１７、信号処理装置１１、データ暗号化器６、ＩＰデータグラム構成器１６の他、キー暗号化器１３０およびキー変換器１３２を有している。キー暗号化器１３０は、マスターキー１２０とワークキー１２１から暗号化したキー１２３を生成する。暗号化したキー１２３が変復調器（モデム）１７を経由して受信装置２の変復調器（モデム）２７で受信される。ＩＰデータグラム構成器１６は伝送すべきデータ５に、暗号化伝送データの送信先である受信装置２の宛先アドレスおよび暗号化処理を行うか否かを示すフラグを有するＩＰヘッダ１４を付加してＩＰデータグラム１５を構成する。ＩＰヘッダ１４の宛先アドレスは、キー変換器１３２に入力され、ワークキー１２１とともにキー変換器１３２において暗号鍵（暗号化セッションキー）７を生成するのに使

用される。このように、暗号鍵７は、ワークキー１２１の他に、受信装置２の宛先アドレスを元にして生成されているので、正当な受信装置２以外で暗号化伝送データを受信したとしても、正当に復号できないことになる。この詳細は後述する。キー変換器１３２で生成された暗号鍵（セッションキー）７が暗号化器６において伝送すべきデータ５を暗号化するのに使用される。暗号化器６において暗号化され大容量伝送路１２に送出されるデータが暗号化データ１９である。暗号化データ１９は、伝送すべきデータ５を暗号化したデータに、暗号化されていないＩＰヘッダ１４が付加されて、図示しない送信手段によって大容量伝送路１２に送出される。

【００３１】受信装置２は、小容量伝送路１３に接続された変復調器（モデム）２７、信号処理装置２１、ＩＰデータグラム分解器２６、データ復号器９の他に、キー復号器２３０、キー変換器２３２を有している。キー復号器２３０は変復調器（モデム）２７を経由して受信した暗号化されているキー１２３をマスターキー２２０を用いてワークキー２２１を復号する。ＩＰデータグラム分解器２６は、暗号化データ１９からＩＰヘッダ１４を分離し、受信装置２の宛先アドレスを取り出し、キー変換器２３２に印加する。キー変換器２３２は、宛先アドレスと、復号されたワークキー２２１から復号鍵（復号用セッションキー）８を変換する。本実施例においては、宛先アドレスをも用いて復号鍵８を再生しているから、正当なアドレスでない受信装置においては正当な復号鍵が生成できない。なお、本実施例における宛先アドレスは単一の装置の宛先アドレスだけを意味するだけでなく、複数の受信装置から構成されるグループを意味（指定）することができる。その場合、上述した暗号化処理および復号処理は、複数の装置に対する暗号化処理および復号処理を意味する。キー変換器２３２で変換された復号鍵８は大容量伝送路１２を経由して受信した暗号化データ１９を復号するのに使用される。

【００３２】送信装置１におけるマスターキー１２０と受信装置２におけるマスターキー２２０とは実質的に同じ内容である。マスターキー１２０を記録した物体を郵送する等して、送信装置１と受信装置２とでマスターキー１２０（２２０）を共有している。送信装置１はワークキー１２１を生成し、キー暗号化器１３０においてマスターキー１２０を鍵としてワークキー１２１を暗号化し、暗号化したキー１２３を変復調器（モデム）１７を介して小容量伝送路１３に送出し受信装置２に伝送する。また、ワークキー１２１をキー変換器１３２に入力して暗号鍵７に変換し、変換した暗号化鍵（暗号化用セッションキー）７を鍵として、データ暗号化器６において伝送すべきデータ５を暗号化して暗号化データ１９として大容量伝送路１２を介して受信装置２に伝送する。受信装置２において、小容量伝送路１３から受信した暗号化したキー１２３をキー復号器２３０においてマスターキー２２０を用いてワークキー２２１を復号し、キー変換器２３２で復号鍵８に変換し、変換された復号鍵（復号用セッションキー）８を鍵としてデータ復号器９において大容量伝送路１２から受信した暗号化データ１９を復号する。

【００３３】第４実施例のデータ伝送装置の送信装置１におけるワークキーの暗号化処理は、送信装置１と受信装置２の間で既に共有済みの受信装置２が持つ受信端末のシリアルナンバー等の固有情報を鍵（マスターキー）として行えば、受信装置２においてワークキーを得られるように行なわれる。

【００３４】第４実施例においては、暗号化したキー１２３を小容量伝送路１３を経由して伝送するから、ワークキーの漏洩があっても、マスターキー１２０を知らない限り復号鍵８が生成される可能性が殆どないので、鍵伝送の機密性が非常に高い。したがって、大容量伝送路１２を伝送された暗号化データ１９が第３者の受信装置３において正しく復号することが困難であり、情報の漏洩についても安全性がより高かまる。さらに第４実施例においては、送信先の受信装置２の宛先アドレスをも用いて暗号鍵７および復号鍵８の生成（変換）を行うので、正当な受信装置２でしか正当な暗号化器６を生成（再生）できず、かりに暗号化データ１９を受信したとしても正常に暗号化データ１９を復号できない。

【００３５】第４実施例の第１変形例

図９には、好適実施例として、送信装置１においてワークキー１２１を暗号化して暗号化したキー１２３として受信装置２に伝送する例を示したが、第４実施例は、受信装置２の宛先アドレスを用いて暗号鍵７および復号鍵８を変換していて機密性が高くなっているので、ワークキー１２１を小容量伝送路１３を経由して直接、キー変換器２３２における復号鍵（復号化セッションキー）８の変換に使用してもよい。すなわち、図９に図解した送信装置１におけるキー暗号化器１３０、受信装置２におけるキー復号器２３０を削除することができる。この場合、マスターキー１２０、マスターキー２２０の交換をしないで済むので、送信装置１と受信装置２との間の手続きは簡単になる。

【００３６】第４実施例の第２変形例

また、図９を参照して述べた第４実施例は、好適実施例として、送信装置１におけるキー変換器１３２においてワークキー１２１と宛先アドレス１４を用いて暗号化セッションキー７を変換し、その暗号化セッションキー７を用いてデータ１５を暗号化器６において暗号処理する場合を述べたが、第４実施例の簡便な例として、キー変換器１３２において、宛先アドレス１４を用いず、ワークキー１２１のみを用いて暗号化鍵（暗号化セッションキー）７を生成することができる。この場合、キー変換器１３２の構成が簡単になる。同様に、受信装置２におけるキー変換器２３２においても、マスターキー１２０

と同じマスターキー２２０を用いて復号鍵（復号セッションキー）８を生成して、その復号鍵８を用いて受信した暗号化データを復号できる。この場合も、キー変換器２３２の構成が簡単になる。

【００３７】第４実施例の第３変形例

さらに、上述した第４実施例の第１の変形例と第２変形例を組み合わせることもできる。すなわち、第４実施例の第１変形例に従って、図９に図解した送信装置１におけるキー暗号化器１３０、受信装置２におけるキー復号器２３０を削除し、第２変形例に従って、キー変換器１３２およびキー変換器２３２の構成を簡単にする。

【００３８】

【実施例５】本発明のデータ伝送装置の第５実施例を述べる。図１０は本発明のデータ伝送装置の第５実施例の構成図である。第４実施例においては、小容量伝送路１３を用いて、送信装置１から受信装置２に暗号化したキー１２３を伝送したが、第５実施例は、１台の受信装置２が存在しただけのとき、受信装置２から送信装置１に暗号化したワークキー２２３を小容量伝送路１３を経由して伝送し、送信装置１において、暗号化したワークキー２２３からワークキー１２１を復号し、このワークキー１２１から暗号鍵７を変換する。このため、送信装置１には、図９に図解したキー暗号化器１３０に代えてキー復号器２３０と同等のキー復号器１３４が設けられ、受信装置２には、図９に図解したキー暗号化器１３０と同等のキー暗号化器２３４が設けられている。その他の構成および動作は第４実施例と同様である。第５実施例においては、送信装置１に対して受信装置２から暗号化鍵（暗号化用セッションキー）を指定することができる。第５実施例における鍵の機密性、暗号化データ１９の機密性は第４実施例と同等である。

【００３９】第５実施例の変形例

図１０には、好適実施例として、送信装置１においてワークキー１２１を暗号化して暗号化したキー１２３として受信装置２に伝送する例を示したが、第５実施例は、第４実施例と同様、受信装置２の宛先アドレスを用いて暗号鍵７および復号鍵８を変換していて機密性が高いので、ワークキー２２１を小容量伝送路１３を経由して直接、送信装置１のキー変換器１３２における暗号鍵７の変換に使用してもよい。すなわち、送信装置１におけるキー復号器１３４、受信装置２におけるキー暗号化器２３４を削除することができる。この場合、マスターキー１２０、マスターキー２２０の交換をしないで済むので、手続きは簡単になる。その他、第５実施例についても、第４実施例の変形例として述べた種々の簡単な構成をとることができる。

【００４０】

【実施例６】本発明のデータ伝送装置の第６実施例を述べる。第４実施例および第５実施例においては、送信装置１および受信装置２において、好適には、ワークキー１２１と宛先アドレスから、簡便には、第４実施例の変形例として述べたように、ワークキー１２１から暗号鍵（暗号用セッションキー）７を変換するためのキー変換器１３２、および、ワークキー２２１から復号鍵（復号用セッションキー）８を変換するためのキー変換器２３２を設けている。これに対して第６実施例においては、送信装置１のキー変換器１３２の入力を、ワークキー１２１と大容量伝送路１２を用いる伝送における宛先アドレスとし、これらの情報から暗号鍵（暗号用セッションキー）７を生成する。同様に、受信装置２のキー変換器２３２の入力を、ワークキー２２１と受信装置２のアドレスとし、これらの情報から復号鍵（復号用セッションキー）７を生成する。その他の構成および動作は第４実施例と同様である。なお、第６実施例においても、宛先アドレスは単一の装置の宛先アドレスだけを意味するだけでなく、複数の受信装置から構成されるグループを意味（指定）することができる。その場合、上述した暗号化処理および復号処理は、複数の装置に対する暗号化処理および復号処理を意味する。第６実施例においては、第４実施例のようにワークキーのみからセッションキーを生成する方法に対して、宛先アドレスを知らない者にはセッションキーを生成することが困難であるから、鍵の伝送の安全性がより高くなるという利点がある。

【００４１】

【実施例７】本発明のデータ伝送装置の第７実施例を述べる。図１１は本発明のデータ伝送装置の第７実施例の構成図である。データ伝送装置は、大容量伝送路１２および小容量伝送路１３を介して接続される送信装置１と受信装置２とを有する。送信装置１は、暗号化器６およびキー暗号化器１３６を有する。受信装置２は復号器９およびキー復号器２３６を有する。なお図解を簡単するするため、図１１には図５に示したＩＰデータグラム構成器１６およびＩＰデータグラム分解器２６は図示していない。しかしながら、本実施例においても、ＩＰヘッダ１４に規定されている宛先データの処理および暗号処理を行うか否かの処理は上述した実施例と同様に行う。

【００４２】第４実施例では送信装置１から受信装置２に暗号化したキー１２３を小容量伝送路１３を用いて伝送し、第５実施例では受信装置２から送信装置１に暗号化したワークキー２２３を小容量伝送路１３を用いて伝送している。これに対して第７実施例では、送信装置１から受信装置２に暗号化したセッションキー１２４を小容量伝送路１３を用いて伝送する。また、受信装置２が１台の場合は、受信装置２から送信装置１に暗号化したセッションキーを小容量伝送路１３を用いて伝送する。このセッションキーは、大容量伝送路１２を用いた暗号化データ伝送における宛先アドレスに基づいて生成される。

【００４３】送信装置１において暗号化用鍵（暗号化用セッションキー）７を生成し、送信装置１と受信装置２

において共有するマスターキー１２０を鍵としてキー暗号化器１３６を用いて暗号化し、暗号化されたセッションキー１２４を小容量伝送路１３を用いて受信装置２に送る。送信装置１においては、生成した暗号化鍵７を鍵として暗号化器６を用いて伝送すべきデータ５を暗号化して大容量伝送路１２を用いて受信装置２に送る。受信装置２は小容量伝送路１３から受信した暗号化されたセッションキー１２４をマスターキー２２０を鍵として復号器９で復号し、復号鍵（復号用セッションキー）８を得る。受信装置２において、大容量伝送路１２から受信した暗号化データ１９を、上記のようにして求めた復号鍵８を鍵として復号器９で復号する。第７実施例は、直接、暗号化したセッションキー１２４を送信装置１から受信装置２に伝送しているので、送信装置１および受信装置２におけるキー変換器１３２およびキー変換器２３２が不要であるという構成上の利点がある。

【００４４】

【実施例８】本発明のデータ伝送装置の第８実施例を述べる。図１２は本発明のデータ伝送装置の第８実施例の構成図である。送信装置１はＩＰデータグラム構成器１６および暗号化器６を有する。受信装置２は復号器９およびＩＰデータグラム分解器２６を有する。送信装置１において、伝送すべきデータ５がＩＰデータグラム構成器１６に入力されてＩＰヘッダ１４が付加されてＩＰデータグラム１５が形成される。暗号化器６はＩＰヘッダ１４に含まれる宛先データも暗号化する。ＩＰヘッダ１４のデータも暗号化したデータ１９が大容量伝送路１２を経由して受信装置２に伝送される。受信装置２は、大容量伝送路１２から受信したＩＰヘッダ１４のデータも暗号化したデータ１９の全てを復号器９において復号する。それにより、ＩＰデータグラム１５も復号される。ＩＰデータグラム分解器２６が復号したＩＰデータグラム１５を分解してＩＰヘッダ１４を取り出し、この中の宛先アドレスを見て、それが自分宛のデータであるか否かを知り、自分宛のデータである場合には、ＩＰヘッダを取り除いたもとのデータ部分を取り出す。なお、本実施例において、小容量伝送路１３を用いた送信装置１と受信装置２との間の暗号鍵または暗号鍵を生成するための情報の授受、あるいは、送信装置１と受信装置２との間で復号鍵または復号鍵を生成するための情報の授受は、上述した第１～第７実施例のいずれも適用できる。すなわち、本実施例は、ＩＰヘッダ１４も暗号化の対象にした例を示しており、小容量伝送路１３を用いた暗号鍵または復号鍵の伝送方法は上述した実施例のいずれも適用できる。本実施例においては、送信装置１または受信装置２において、伝送されているデータを暗号化あるいは復号するかしないかの判断を省略することができる。

【００４５】変形例

上述した実施例は全て、インターネット・プロトコルＩＰを用いた場合について例示したが、本発明の実施に際しては、インターネット・プロトコルＩＰに限定されず、その他の伝送プロトコル、たとえば、ＡＴＭ（Asynchronous Transfer Mode、非同期転送モード）に従うプロトコルなどを用いることができる。また本発明の実施に際しては、上述した種々の実施例を適宜組み合わせることができる。

【００４６】

【発明の効果】本発明によれば、データを伝送する大容量伝送路（第１の伝送系統）とは異なる小容量伝送路（第２の伝送系統）を用いて暗号化あるいは復号の処理のための鍵あるいはこの鍵を生成するための情報を伝送して鍵の伝送の機密性を高めており、大容量伝送路を介して伝送される暗号化データの漏洩に対して安全性が高くなる。特に、本発明においては、制御情報として宛先データを付加しているので、正当な受信装置（第２の伝送装置）においてのみ有効に暗号化データが復号可能となる。また本発明においては、鍵を暗号化して伝送できるので、鍵の漏洩に対する安全性が一層高まる。

【００４７】また本発明によれば、伝送のために必要な制御情報を見るだけで暗号化、復号の必要性が判別できる。

【図面の簡単な説明】

【図１】図１は伝送路上のデータを暗号化する伝送方法の一例を示す概略図である。

【図２】図２は本発明のデータ伝送装置の第１実施例の構成を示す概略図である。

【図３】図３は本発明の実施例のデータ伝送装置における大容量伝送路および小容量伝送路の具体的構成を示す図である。

【図４】図４はインターネット・プロトコルＩＰにおけるメッセージ伝送の単位であるＩＰデータグラムの概略図である。

【図５】図５は図２に図解した本発明のデータ伝送装置の第１実施例についてインターネット・プロトコルＩＰを適用して実現したより詳細な構成を示す図である。

【図６】図６は本発明のデータ伝送装置の実施例における送信装置の動作処理を示すフローチャートである。

【図７】図７は本発明のデータ伝送装置の実施例における受信装置の動作処理を示すフローチャートである。

【図８】図８は本発明のデータ伝送装置の第３実施例の概略構成図である。

【図９】図９は本発明のデータ伝送装置の第４実施例の構成図である。

【図１０】図１０は本発明のデータ伝送装置の第５実施例の構成図である。

【図１１】図１１は本発明のデータ伝送装置の第７実施例の構成図である。

【図１２】図１１は本発明のデータ伝送装置の第８実施例の構成図である。

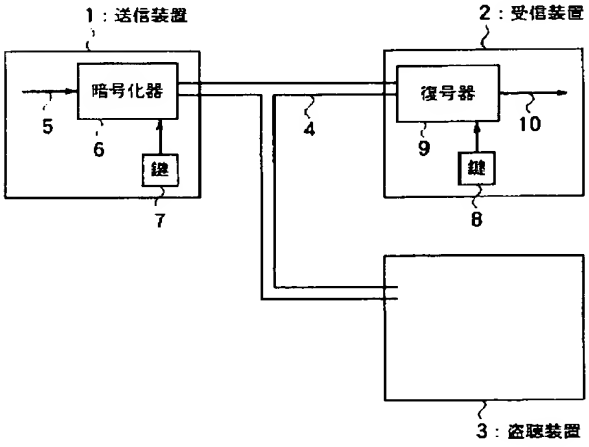
19

【符号の説明】
１・・送信者　２・・受信者　３・・盗聴受信装置
５・・伝送すべきデータ
６・・暗号化器　７・・暗号鍵（暗号化用セッションキー）
８・・復号鍵（復号化用セッションキー）
９・・復号器
１２・・大容量伝送路（衛星回線伝送路）
１３・・小容量伝送路（公衆電話回線）

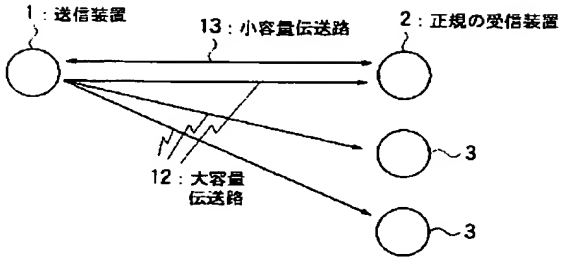
20

１４・・ＩＰヘッダ
１５・・ＩＰデータグラム
１６・・ＩＰデータグラム構成器　２６・・ＩＰデータグラム分解器
１７、２７・・変復調器（モデム）
１９・・暗号化データ
１２０，２２０・・マスターキー
１２１，２２１・・ワークキー
１２３，２２３・・暗号化したキー

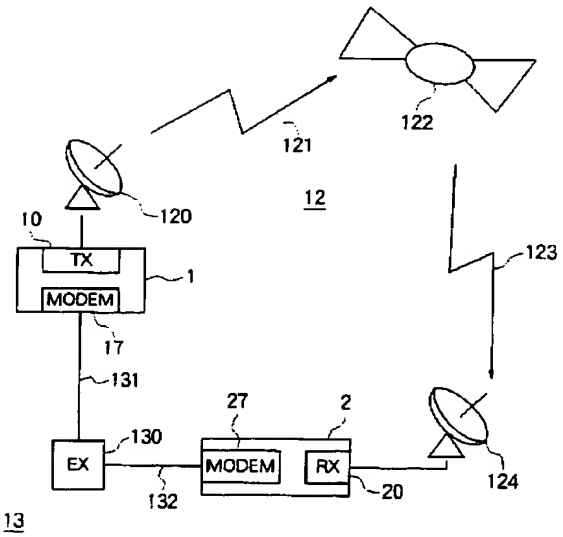
【図１】



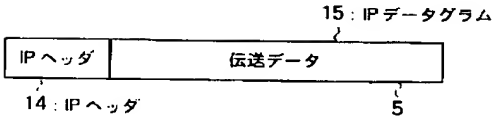
【図２】



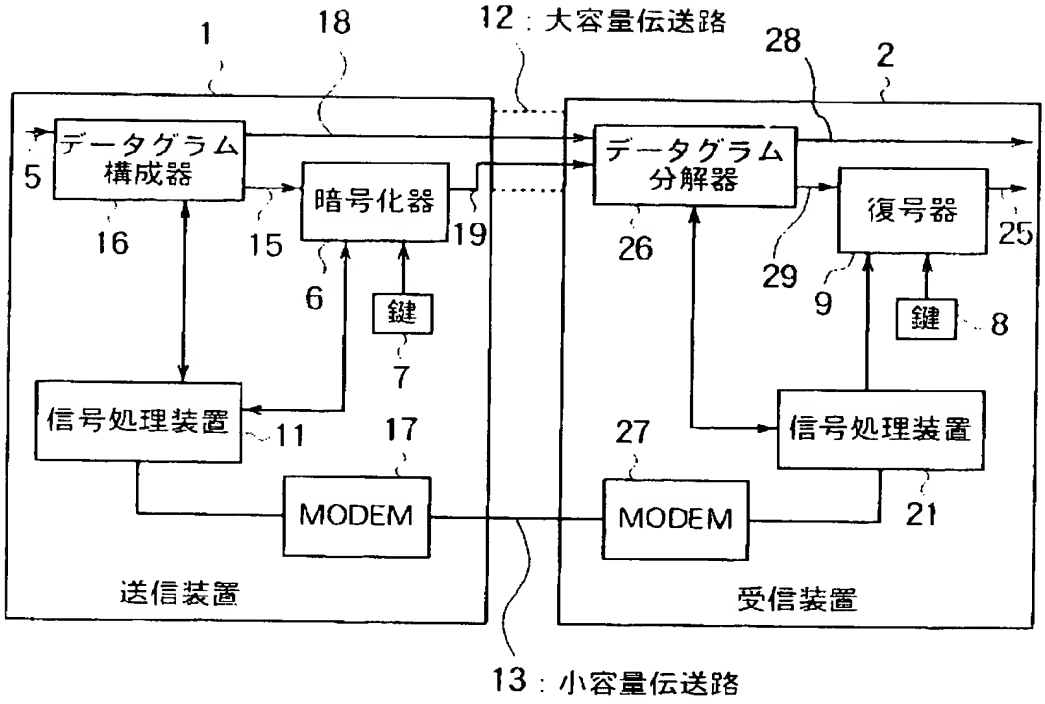
【図３】



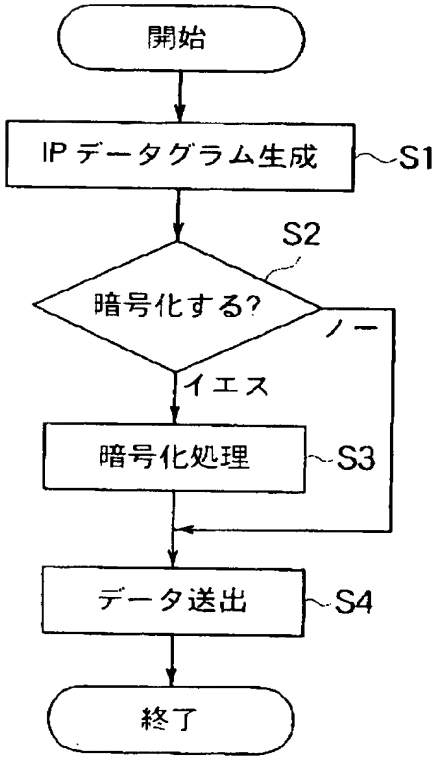
【図４】



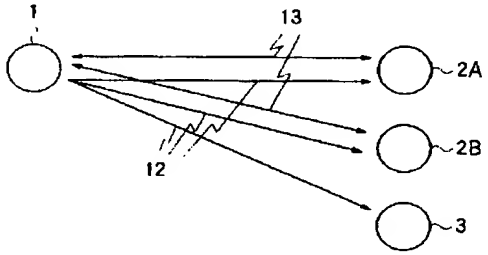
【図５】


12：大容量伝送路
1
18
28
2
データグラム構成器
5
暗号化器
19
データグラム分解器
復号器
25
16
15
26
29
9
6
鍵
8
7
信号処理装置
11
17
27
信号処理装置
MODEM
MODEM
21
送信装置
受信装置
13：小容量伝送路

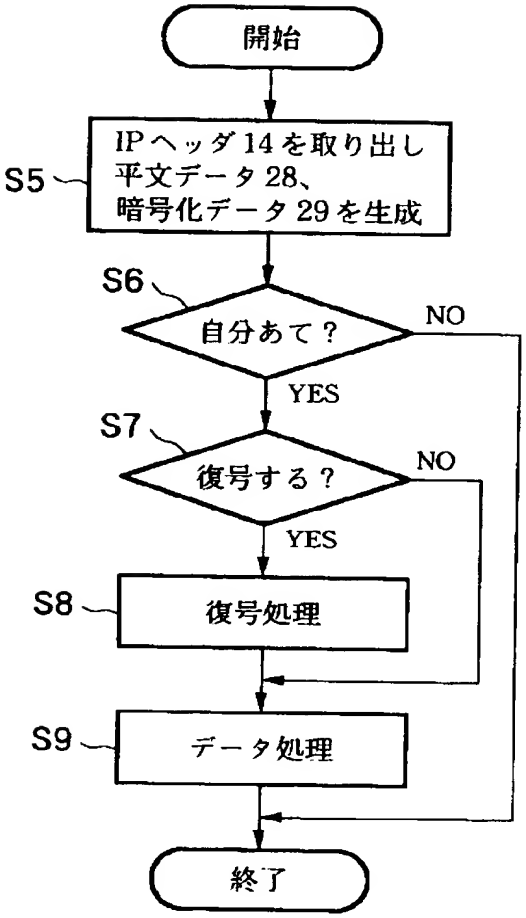
【図６】


開始
IP データグラム生成
S1
S2
暗号化する?
ノー
イエス
暗号化処理
S3
データ送出
S4
終了

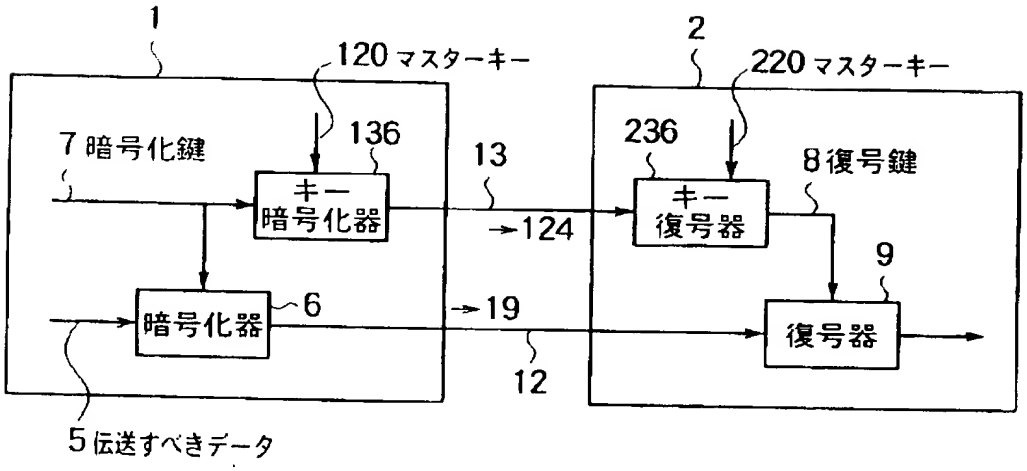
【図８】


1
13
2A
2B
12
3

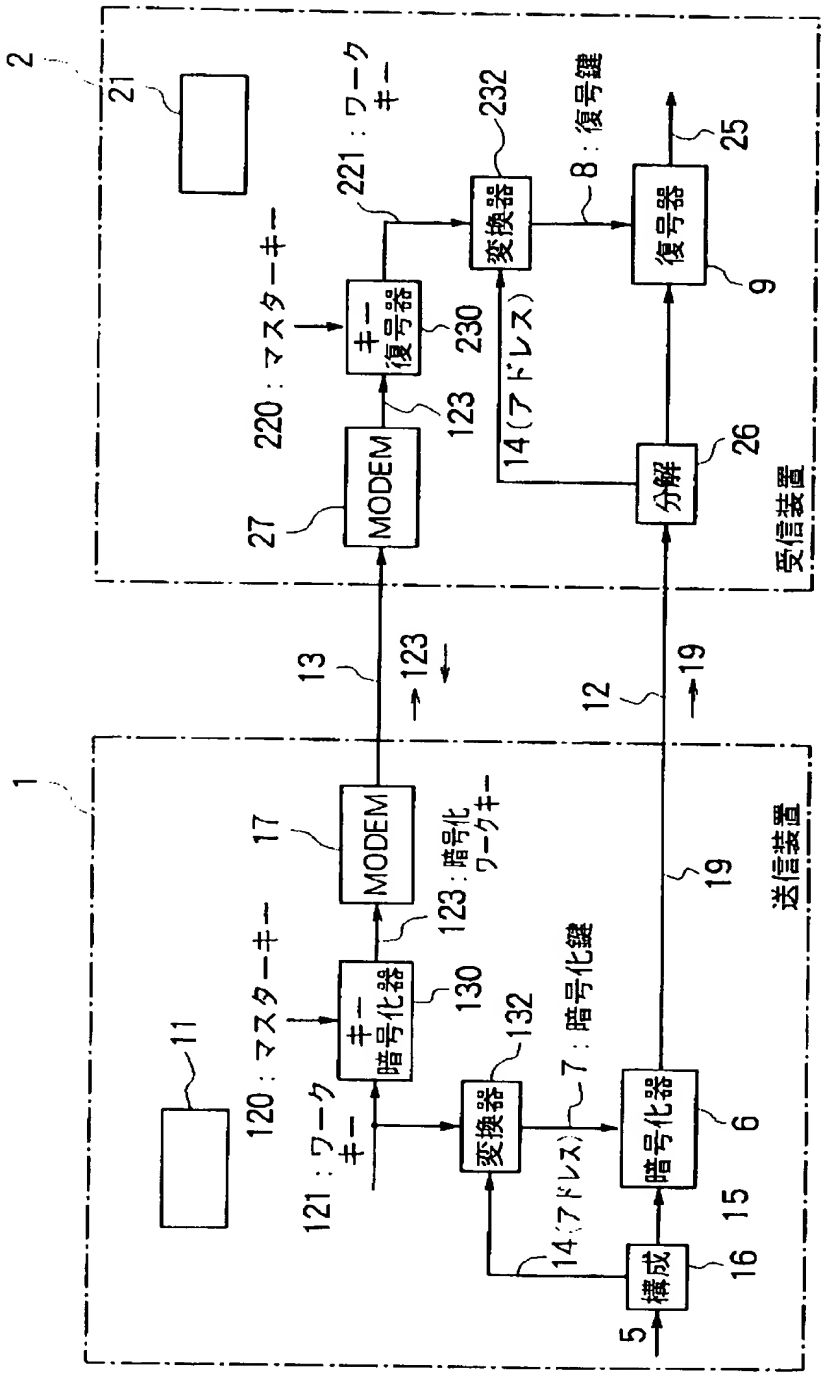
【図７】


開始
IPヘッダ14を取り出し
平文データ28、
暗号化データ29を生成
S5
S6
自分あて？
NO
YES
S7
復号する？
NO
YES
S8
復号処理
S9
データ処理
終了

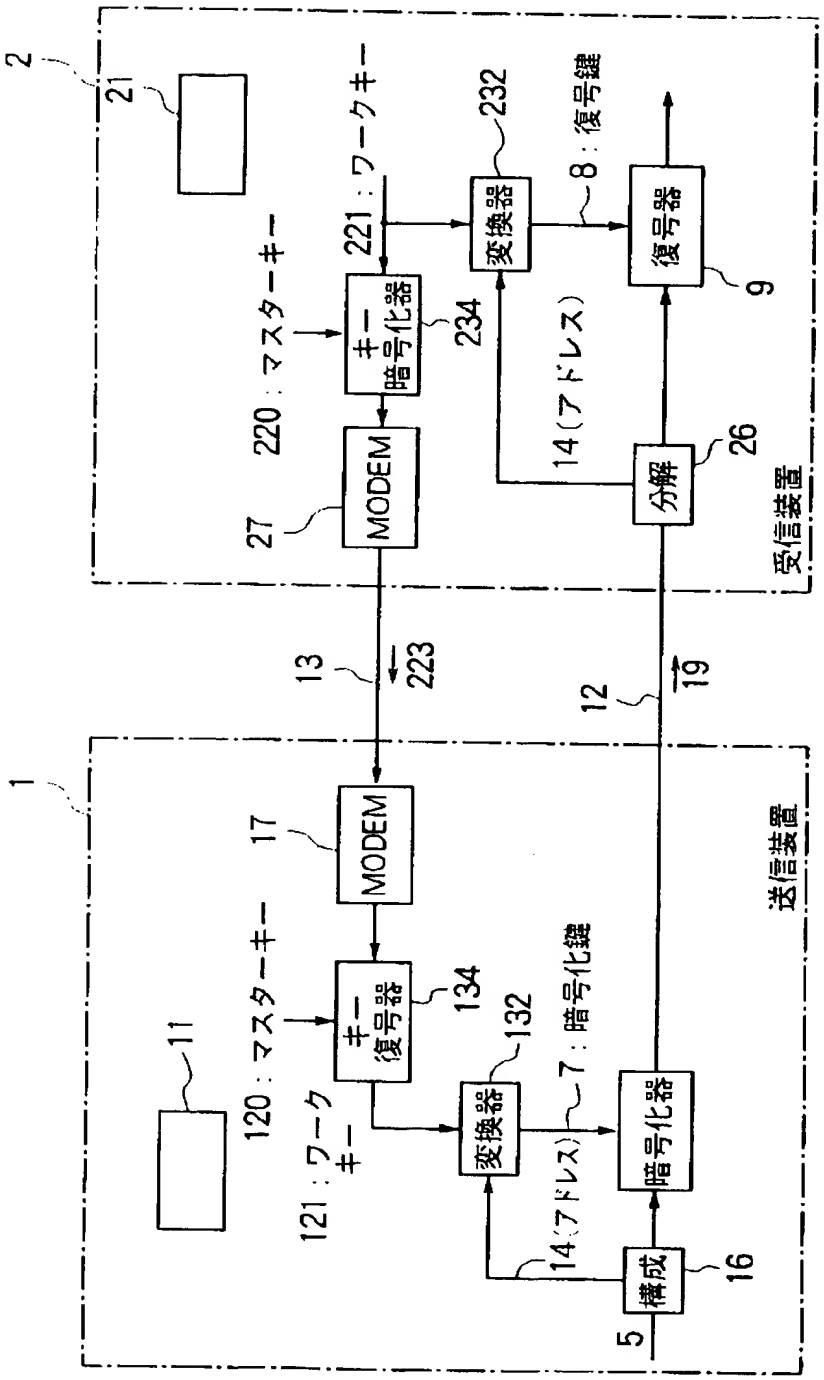
【図１１】


1
120 マスターキー
2
220 マスターキー
7 暗号化鍵
136
キー
暗号化器
13
→124
236
キー
復号器
8 復号鍵
9
暗号化器
6
→19
復号器
12
5 伝送すべきデータ

【図９】


2
21
221：ワーク
キー
232
8：復号鍵
25
変換器
復号器
9
キー
復号器
230
220：マスターキー
123
14（アドレス）
分解
26
27
MODEM
受信装置
13
123
12
19
1
17
MODEM
123：暗号化
ワークキー
19
送信装置
120：マスターキー
キー
暗号化器
130
132
7：暗号化鍵
11
121：ワーク
キー
変換器
暗号化器
6
14（アドレス）
15
構成
16
5

【図１０】


2
21
232
8：復号鍵
221：ワークキー
変換器
復号器
9
キー暗号化器
234
220：マスターキー
14（アドレス）
MODEM
27
分解
26
受信装置
13
223
12
19
1
MODEM
17
送信装置
キー復号器
134
120：マスターキー
11
132
7：暗号化鍵
121：ワークキー
変換器
暗号化器
14（アドレス）
構成
16
5

【図１２】